

SECURE COMMUNICATIONS

ABSTRACT

A method of providing secure communications between a first and a
5 second communications unit comprising a key exchange between the
communications units resulting in a shared secret key, the key exchange
including a user interaction. The method includes the steps of providing, at
least partly by means of a user interaction, a passcode to the first and
second communications units; generating a first contribution to the shared
10 secret key by the first communications unit and a second contribution to the
shared secret key by the second communications unit, and transmitting each
generated contribution to the corresponding other communications unit;
authenticating the transmitted first and second contributions by the
corresponding receiving communications unit based on at least the
15 passcode; and establishing said shared secret key by each of the
communications units from at least the corresponding received first or
second contribution, only if the corresponding received contribution is
authenticated successfully.